## REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-30 are pending in the application. The Examiner additionally stated that claims 1-30 are rejected. By this communication, claims 1, 10, 19, 24-25, and 29 are amended. Hence, claims 1-30 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

**Information Disclosure Statements**

The Examiner noted that The information disclosure statements filed on 04/16/04 and 07/25/06 fail to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication, or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. The Examiner remarked that the statements have been placed in the application file, but the information referred to therein has not been considered.

In reply, Applicant appreciates the Examiner's diligence in ensuring that the information disclosure statements comply with the Rules, and notes that the references associated with the noted non-compliant submissions were filed in a compliant information disclosure statement submitted on 05/30/2007.

**In the Specification**

The Examiner objected to the disclosure because of the following informalities:

The Examiner noted the use of acronyms (i.e., IEEE, RSA, USB, etc.) throughout the specification without first including a description in plain text as required.

The disclosure was objected to because it contains an embedded hyperlink and/or other form of browser-executable code. The Examiner required Applicant to delete the embedded hyperlink and/or other form of browser-executable code per MPEP 608.01.

The Examiner also noted the use of the trademark Linux® in the application, and stated that it should be capitalized wherever it appears and be accompanied by the generic terminology. The Examiner further pointed out that although the use of trademarks is

permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Appropriate correction was required.

In reply, Applicant has amended the specification to first provide a description in plain text of all acronyms that are used. Applicant has in addition amended the specification to delete the embedded hyperlink and to capitalize "LINUX" and to accompany such use with generic terminology.

Accordingly, it is requested that the objections to the specification be withdrawn.

In addition, Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

**In the Claims**

**Claim Objections**

The Examiner objected to claims 10, 24, and 29 because the acronym "x86" is employed without first including a description in plain text as required.

In reply, Applicant respectfully traverses and notes that "x86" is not an acronym, but a well-known term of art that describes a particular instruction set architecture which runs on x86-compatible microprocessors. However, in a good faith effort to further prosecution of this application through the Office, Applicant has amended claims 10, 24, and 29 to recite "the instruction format for execution on an x86-compatible microprocessor" in place of "the x86 instruction format."

Consequently, it is requested that the objections to claims 10, 24, and 29 be withdrawn.

**Rejections Under 35 U.S.C. §102(b)**

The Examiner rejected claims 1-9, 11-13, 15-23, 25-28, and 30 under 35 U.S.C. 102(e) as being anticipated by Yup et al. (2002/0191784). Applicant respectfully traverses the Examiner's rejections.

- a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that an intermediate result (*data blocks*) be generated [page 3, paragraph 0039];
- and execution logic (*transformation blocks*), operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations, configured to generate said intermediate result [page 3, paragraph 0039].

In reply, Applicant respectfully disagrees with the Examiner's characterization of Yup vis-à-vis that subject matter which is recited in claim 1. To aid in the following analysis, claim 1, as amended herein, is repeated below.

1. An apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by a microprocessor as part of an instruction flow executing on said microprocessor, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that an intermediate result be generated; and

execution logic, operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations, and configured to generate said intermediate result.

Applicant respectfully asserts that Yup et al. do no teach a cryptographic instruction. In fact, Applicant has been careful to search Yup et al. and asserts that the term "cryptographic instruction" cannot be found. Yup et al. teach "A circuit includes a single circuit portion for implementing the Advanced Encryption Standard (AES) block cipher algorithm in a system having a plurality of channels. The circuit portion includes a circuit for individually generating, on the fly, the round keys used during each round of the AES block cipher algorithm. The circuit portion also includes shared logic circuits

that implement the transformations used to encrypt and decrypt data blocks according to the AES block cipher. The single circuit portion encrypts or decrypts data blocks from each of the plurality of system channels in turn, in round-robin fashion. The circuit portion also includes a circuit for determining S-box values for the AES block cipher algorithm. The circuit additionally implements an efficient method for generating round keys on the fly for the AES block cipher decryption process. (Abstract)

It is clear that Yup et al. teach a circuit for implementing the AES block cipher algorithm in a system having a plurality of channels. This technique is in part analogous to conventional stand-alone cryptographic processing units, the problems of which the present inventors have noted and for which the present invention is provided to overcome. Yup et al. are utterly silent with regard to how their invention is commanded or directed to process data blocks other than to present a plurality of input registers 102 and associated control signals 103 that are coupled to a corresponding plurality of "system channels."

One skilled will appreciate that this type of configuration is quite disadvantageous in that to provide for encryption and/or decryption of data, or other cryptographic operations, a processor must provide for communication with Yup et al.'s device via some system channel mechanism.

On the other hand, claim 1 recites a cryptographic instruction that is received by a microprocessor as part of an instruction flow executing on said microprocessor. The claim continues to recited how the cryptographic instruction prescribes that an intermediate result be generated. Yup et al. do not teach or suggest an instruction that provides for the foregoing limitation. The claim also recites execution logic, operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations, and configured to generate said intermediate result. Although Yup et al. teach data block, as the Examiner suggests, such a block is not operatively coupled to a cryptographic instruction, nor is its generation directed responsive to receipt of a cryptographic instruction received by an microprocessor. In fact, Yup et al. are utterly silent in this regard.

Based upon the above arguments, Applicant respectfully requests that the rejection of claim 1 be withdrawn.

With respect to claims 2-9, 11-13, and 15-18, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Yup et al. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-9, 11-13, and 15-18.

As per claim 19, the Examiner noted that Yup et al. disclose an apparatus for performing cryptographic operations, comprising:

- a control word, configured to prescribe that an intermediate result(*data blocks*) be generated during execution of one of the cryptographic operations (*noting that transformations are then repeated on the data block that is fed back until a predetermined number of rounds is completed*) [page 4, paragraph 0040-0041]. The examiner noted that it is inherent to employ a current round number if the apparatus is comparing the current round number to a predetermined round number; and
- a cryptography unit (*transformation blocks*) within a device, configured to execute said one of the cryptographic operations responsive to receipt of a cryptographic instruction.

Applicant respectfully disagrees with the Examiner's arguments provided above and directs attention to the arguments submitted in traversal of the rejection of claim 1. In summary, Yup et al.'s invention is a stand-alone unit, not part of a microprocessor. As such, it does not execute an instruction flow. And furthermore, the instruction flow does not provide a cryptographic instruction that prescribes, *inter alia*, that an intermediate result be generated when executing said one of the cryptographic operations.

In view of the above arguments, it is respectfully requested that the rejection of claim 19 be withdrawn.

With respect to claims 21-23, these claims depend from claim 19 and add further limitations that are neither anticipated nor made obvious by Yup et al. Accordingly,

Applicant respectfully requests that the Examiner withdraw the rejections of claims 21-23.

As per claim 25, the Examiner noted that Yup et al. disclose a method for performing cryptographic operations in a device, the method comprising:

- a. via a cryptographic instruction, prescribing that an intermediate result be generated during execution of one of a plurality of cryptographic operations (noting that transformations are then repeated on the data block that is fed back until a predetermined number of rounds is completed) [page 4, paragraphs 0040-0041]; and
- receiving the cryptographic instruction, and generating the intermediate result when executing the one of the cryptographic operations (noting transformations are then repeated on the data block that is fed back until a predetermined number of rounds is completed) [page 4, paragraph 0040-0041].

Applicant respectfully disagrees with the points asserted above and directs the Examiner's attention to the arguments submitted in traversal of the rejections of claims 1 and 19. Claim 25 recites, among other elements and limitations, within a microprocessor, receiving a cryptographic instruction that prescribes that an intermediate result be generated during execution of one of a plurality of cryptographic operations. As noted earlier, Yup et al. does not teach a microprocessor, nor it is taught that the microprocessor receives a cryptographic instruction that prescribes that an intermediate result be generated during execution of one of a plurality of cryptographic operations. This is because Yup et al. teaches a stand-alone AES unit that is fed data from system channels.

Accordingly, it is respectfully requested that the rejection of claim 25 be withdrawn.

With respect to claims 26-28 and 30, these claims depend from claim 25 and add further limitations that are neither anticipated nor made obvious by Yup et al. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 26-28 and 30.

**Rejections Under 35 U.S.C. §103(a)**

The Examiner rejected claims 10, 14, 24, and 29 under 35 U.S.C. 103(a) as being unpatentable over Yup et al.. Applicant respectfully traverses the Examiner's rejections and notes that claims 10, 14, 24, and 29 depend from claims 1, 19, and 25, as appropriate, and recite limitations above and beyond those elements which have been argued above as being allowable over the prior art of record. Consequently, Applicant respectfully requests that the Examiner withdraw the rejections of claims 10, 14, 24, and 29.

## CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-30 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,
**HUFFMAN PATENT GROUP, LLC**

/Richard K. Huffman/

By: _____

**RICHARD K. HUFFMAN, P.E.**
Registration No. 41,082
Tel: (719) 575-9998

08/23/2007

Date: _____